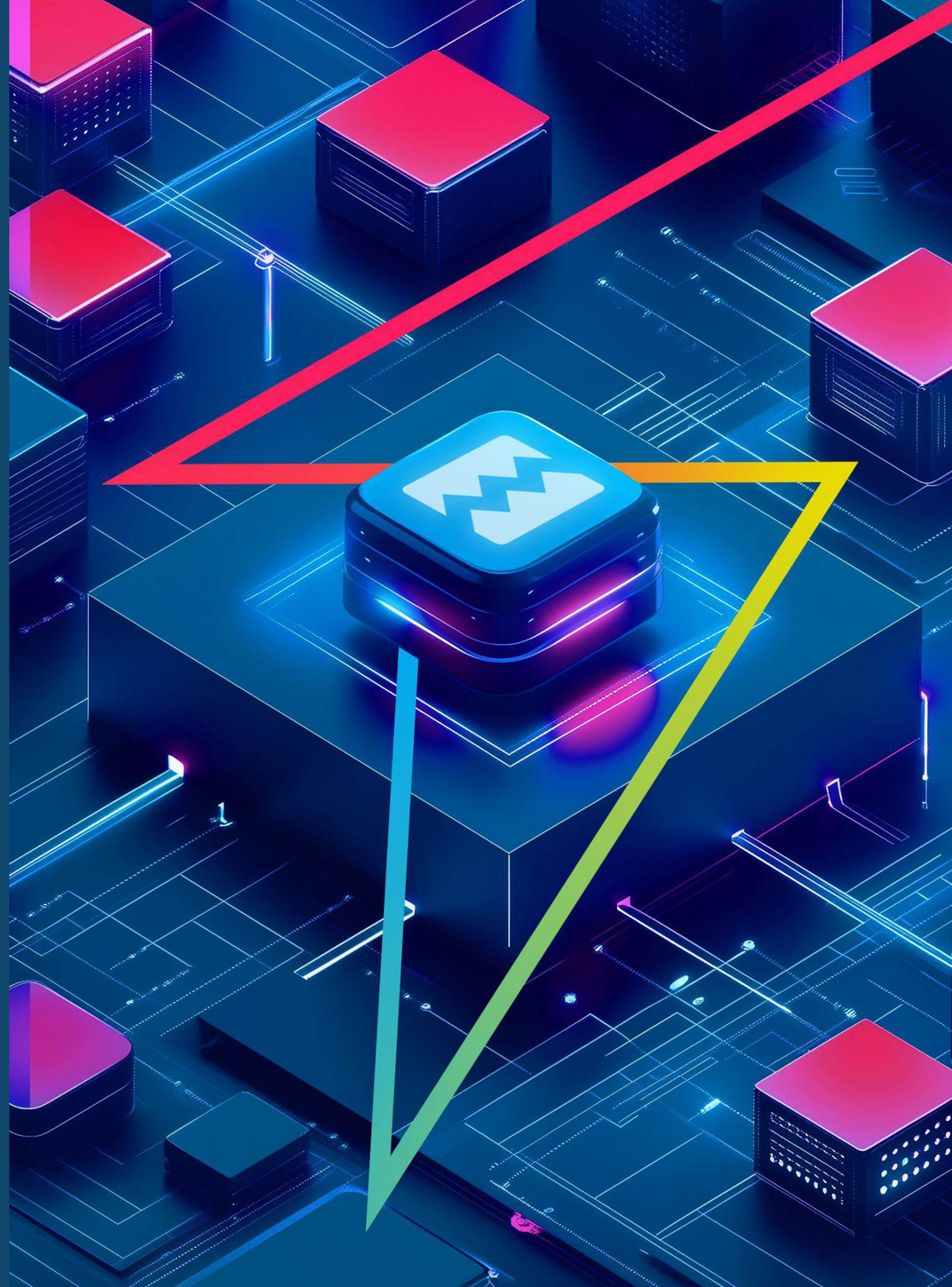
xello

Способы обнаружения кибератак с помощью киберобмана

Черников Дмитрий

Руководитель направления технического сопровождения продаж



О компании

Xello — лидер сегмента решений класса Distributed Deception Platform (DDP) на российском рынке информационной безопасности

50+

проектов реализовали в различных сферах экономики

5+

лет разрабатываем первую российскую платформу кибероблана

Кибератаки в 2024

xello

мая, 23:18 / Бизнес

Причиной сбоя в работе СДЭК мог стать вирус-шифровальщик

Восстановление доставки зависит от того, как часто компания делала бэкапы, отмечают эксперты

Лиана Липанова

Прочту позже

Евгений Разумный / Ведомости

В работе ретейлера «Верный» произошел сбой из-за атаки хакеров

Андрей Злобин
Редакция Forbes

Копировать ссылку

Фото Сергея Елагина / Бизнес Online / ТАСС

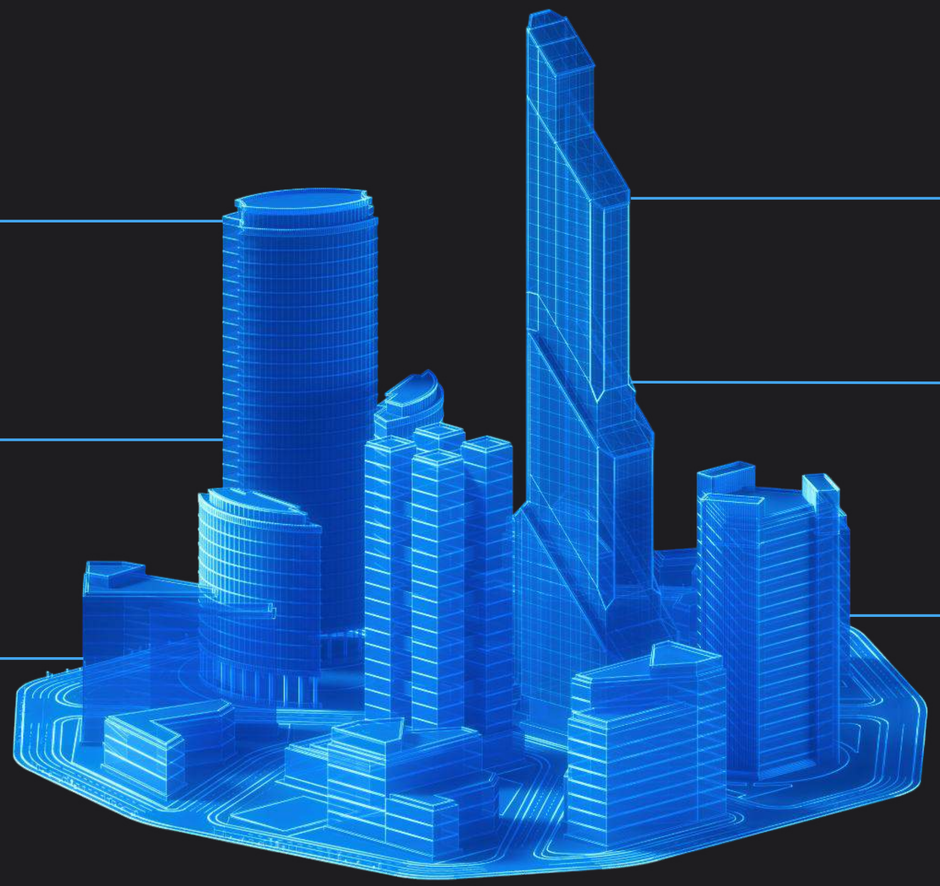
Почему атаки успешны

xello

Облачная инфраструктура

Подрядчики

Внутренняя разработка



Сотрудники

Уязвимости

Промышленный сегмент

Актуальность

xello

4 шага

в среднем требуется,
чтобы получить доступ
во внутреннюю сеть компании

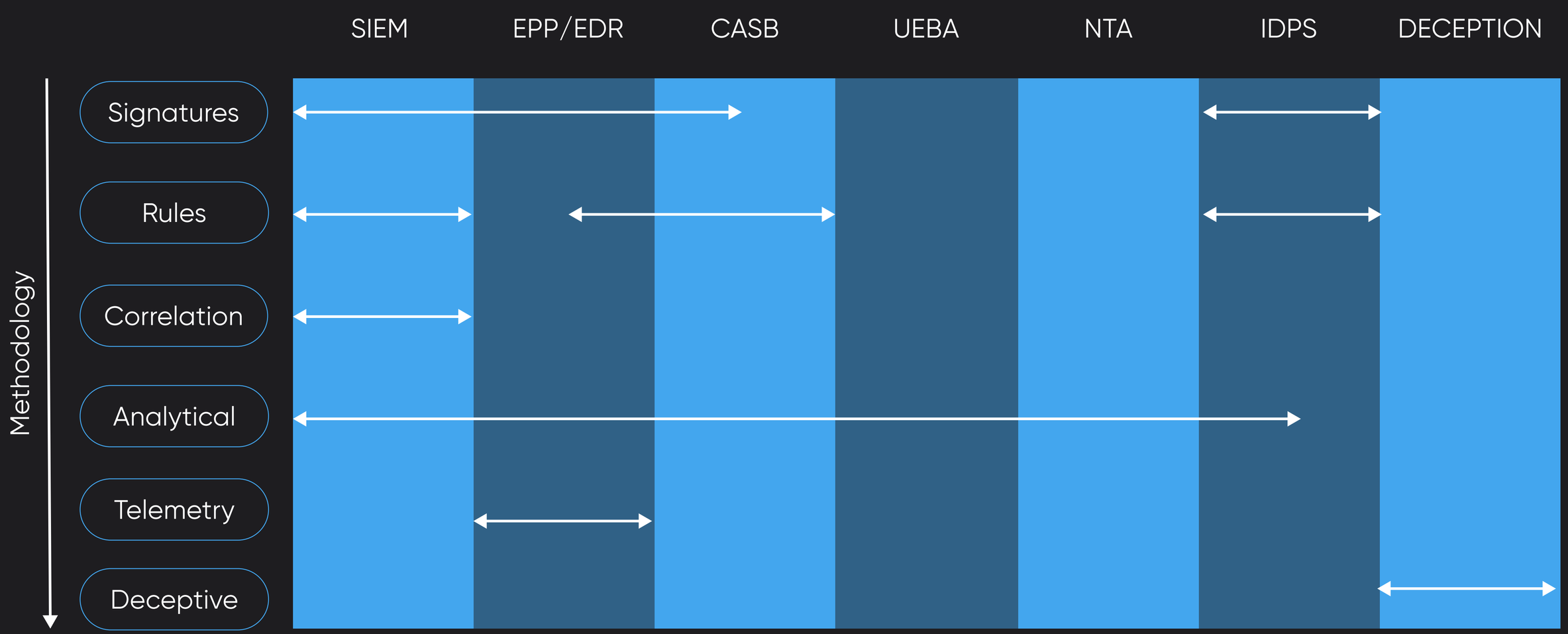
10 дней

медианное время незаметного
присутствия злоумышленника
в инфраструктуре в 2023 г.

Итоги пентестов 2023 // Positive Technologies
M-Trends 2024 // Mandiant (Google Cloud Security)

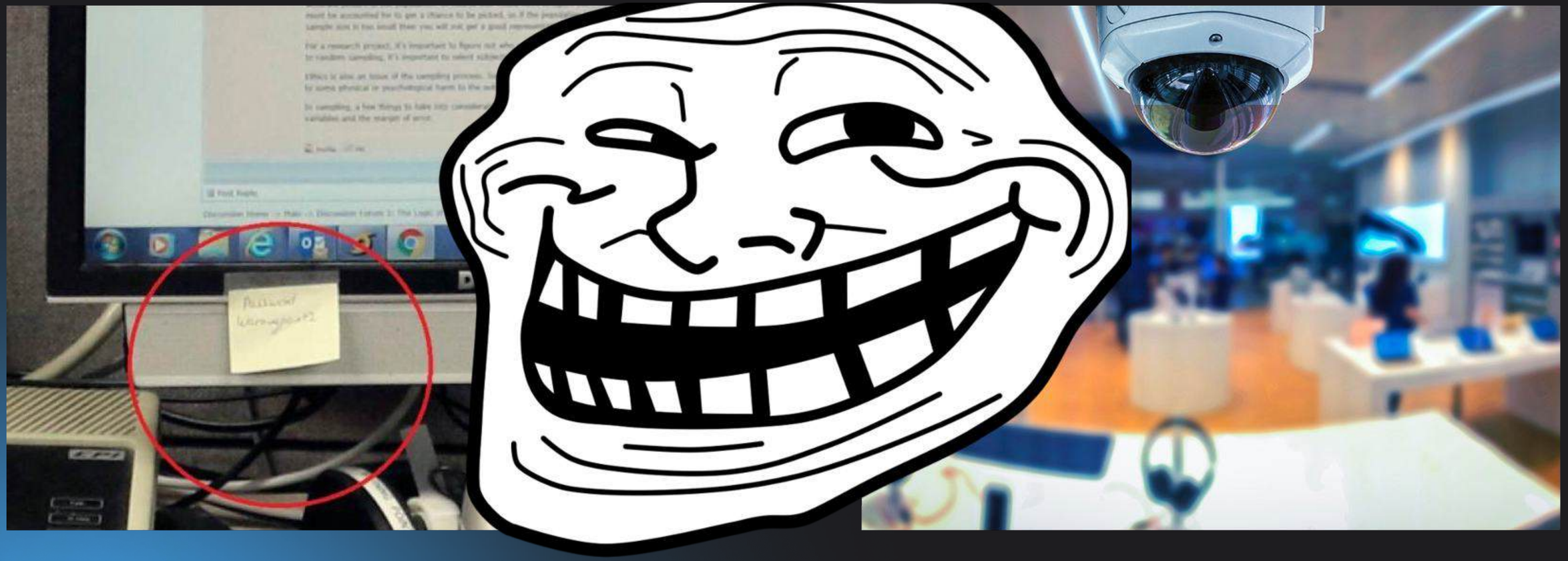
Техники детекта

xello



Доступные инструменты для создания ложного слоя

xello



Доступные инструменты для создания ложного слоя

xello

Пользовательский сегмент

- Заведение фейковых администраторов в Active Directory – (GitHub: samratashok/Deploy-Deception: A PowerShell // DEJAVU)
- Canarytokens
- Инжекция ложных УЗ в сетевую память (для ОС Windows)
- Обманываем BloodHound

Доклад: Десептим
от видеокамеры до бладхаунда

Доступные инструменты для создания ложного слоя

xello

Корпоративная сеть — Open Source-ловушки

- HONEYD
- COWRIE
- DIONAEA
- HONEYTRAP
- и другие...

Доклад: Варианты Open Source-ловушек, фреймворки по их управлению и мониторингу

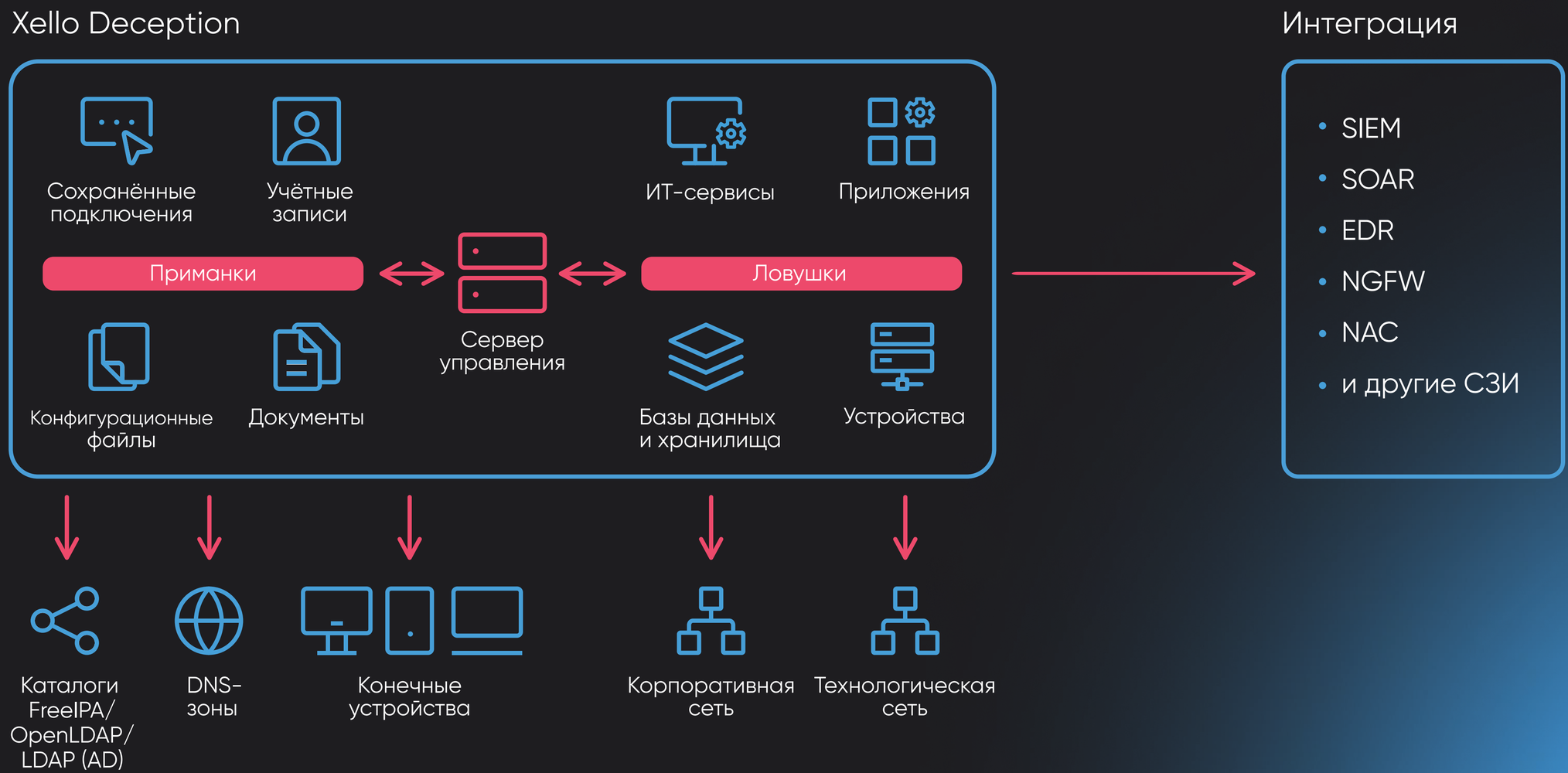
Новые типы действий в арсенале защитников

xello

Действия киберобмана	Описание
launch_decoy	Создание и развертывание пользовательских ложных целей. Дополнительные действия включают создание учётных данных decoy_ser или plant_creds на реальных хостах для заманивания злоумышленника.
ping_responder	Ответ на запрос ping, даже если цели не существует на этом адресе.
portspoof	Фальсификация портов и сервисов на реальных или ложных хостах.
falsify_response	Фальсификация уведомления об успехе или неудаче для попыток входа в систему или получения информации.
traffic_control	Изменение скорости траффика, что приводит к задержке злоумышленника или его неуспеху.
TCP_reset	Отключение сетевого соединения. Задержка или сдерживание злоумышленника.
create_user	Создание ложных учётных записей для заманивания злоумышленника на ложные сервисы.
plant_creds	Распространение ложных учётных данных для истощения ресурсов злоумышленника или его заманивания на ложные сервисы.

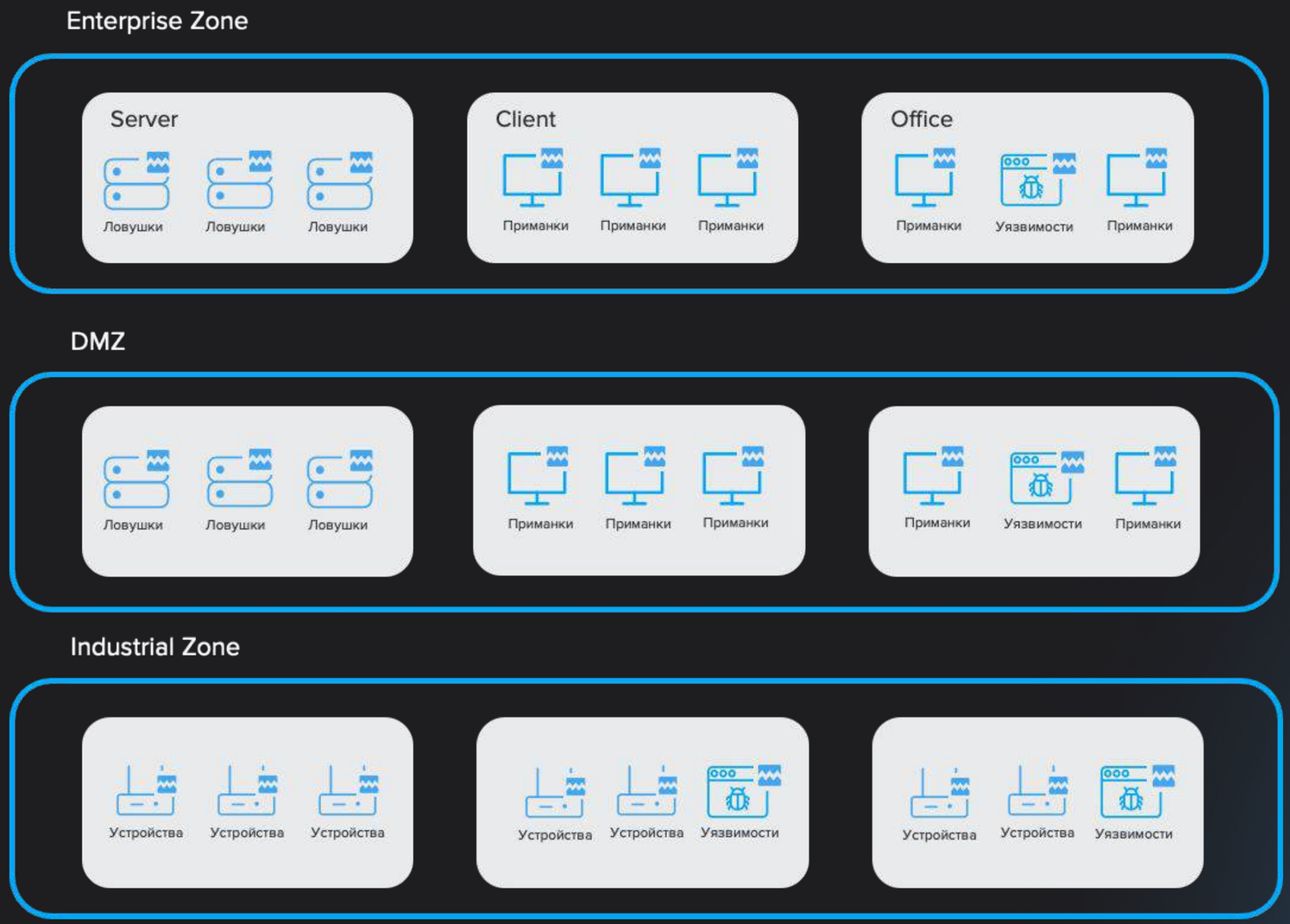
Как работают современные системы киберобмана

xello



Подходы к внедрению кибероbмана

xello



xello

Ответим
на ваши вопросы!

sales@xello.ru

+7 (499) 842 90 90